MATH 204B, WINTER [redacted]

NUMBER THEORY II, HW 1

[redacted].

From Neukirch's book `Algebraic Number Theory`:

- Exercises:

  3 on page 106; 1 and 2 on page 115

Problem A. Let $|\cdot|_1, |\cdot|_2, \ldots, |\cdot|_n$ be non-trivial inequivalent absolute values on a field K.

(a) Show that there is an element $a \in K$ with the following properties:

$$|a|_1 > 1, \quad |a|_2 < 1, \quad \ldots, \quad |a|_n < 1.$$

(`Hint`. Induction on n. For $n = 2$ use that the open unit ball for $|\cdot|_1$ at 0 is not contained in that of $|\cdot|_2$, and vice versa.)

(b) Let $a_1, \ldots, a_n \in K$ be arbitrary elements. Prove that for every $\epsilon > 0$ there exists an $x \in K$ such that

$$|x - a_i|_i < \epsilon \qquad \forall i = 1, 2, \ldots, n.$$

(`Hint`. First do the case $a_1 = 1$, $a_2 = \cdots = a_n = 0$ by considering $\frac{a^r}{1+a^r}$ for large enough r. In general try $x = a_1x_1 + \cdots + a_nx_n$ where x_i is close to 1 relative to $|\cdot|_i$ and close to 0 relative to the others.)

Problem B. Consider the ring of p-adic integers $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, thought of as the set of compatible residue classes $(\bar{x}_1, \bar{x}_2, \bar{x}_3, \ldots)$.

(a) Show that $\mathbb{Z}_p$ is a local domain with maximal ideal $\mathfrak{m}_{\mathbb{Z}_p} = (p) = p\mathbb{Z}_p$.

(b) There are (at least) three natural ways to endow $\mathbb{Z}_p$ with a topology:

- Taking the ideals $p^n\mathbb{Z}_p$ to be a neighborhood basis at 0;
- Taking the induced topology from the product $\prod_{n>0} \mathbb{Z}/p^n\mathbb{Z}$;
- The coarsest topology making the maps $\mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$ continuous.

Check that all three give rise to the same topology.

Math 204B, Winter [redacted]

Number Theory II, HW 2

[redacted].

From Neukirch's book `Algebraic Number Theory`:

- Exercises:

  3 and 5 on page 115; 4 on page 123

Problem A. Let K be a field with a non-archimedean absolute value $|\cdot|$.

(a) Let $x, y \in K$. Show that the strong triangle inequality

$$|x+y| \leq \max\{|x|, |y|\}$$

is an equality when $|x| \neq |y|$.

(b) Let $x_1, \ldots, x_n \in K$. Show that

$$|x_1 + \cdots + x_n| = \max\{|x_1|, \ldots, |x_n|\}$$

provided the maximum on the right is achieved exactly once (that is some $|x_i|$ is larger than all $|x_j|$ for $j \neq i$). `Hint:` You may assume $i = 1$, in which case the assumption amounts to the inequality $|x_1| > \max\{|x_2|, \ldots, |x_n|\}$.

Problem B. Let K be a field with a non-trivial non-archimedean absolute value $|\cdot|$, and let $R = \{x \in K : |x| \leq 1\}$ be its valuation ring.

(a) Check that R is integrally closed in its fraction field $\mathrm{Frac}(R) = K$.

(b) Suppose $|K^\times|$ is discrete and choose a uniformizer $\pi \in R$. Explain why every nonzero ideal of R is of the form (π^i) for some $i \geq 0$. Deduce that R is a Dedekind domain.

MATH 204B, WINTER [redacted]

NUMBER THEORY II, HW 3

[redacted]).

From Neukirch's book `Algebraic Number Theory`:

- Exercises:

  4 on page 106; 4 on page 115; 1 on page 123

Problem A. Let K be a field extension of $\mathbb{C}$ with an absolute value $|\cdot|$ extending the ordinary one $|\cdot|_\infty$ on the complex numbers. This exercise shows that $K = \mathbb{C}$.

(a) Suppose there exists an $a \in K\backslash\mathbb{C}$. Show that a has a nearest point in $\mathbb{C}$. That is, there exists a $z_0 \in \mathbb{C}$ for which the inequality

$$|a - z| \geq |a - z_0|$$

is valid for all $z \in \mathbb{C}$.

(b) Replacing a by $a - z_0$, and then scaling by a suitable complex number, show the existence of an $a \in K\backslash\mathbb{C}$ satisfying

$$|a - z| \geq |a| > 1$$

for all $z \in \mathbb{C}$.

(c) For an arbitrary $n \in \mathbb{N}$ use $a^n - 1 = \prod_{i=0}^{n-1}(a - \zeta^i)$ to show that $|a - 1| = |a|$.

(d) Deduce that $|a - n| = |a|$ for all $n \in \mathbb{N}$, and conclude $n \leq 2|a|$. (Contradiction.)

Problem B. Let $(K, |\cdot|)$ be a non-discretely valued non-archimedean field of residue characteristic $p = \text{char}(R/\mathfrak{m}) > 0$. Suppose the p-power Frobenius map $R/(p) \longrightarrow R/(p)$ is surjective[1].

(a) Check that the valuation group $|K^\times|$ is generated by the set of all values $|x|$ in the range $|p| < |x| \leq 1$, and deduce that $|K^\times|$ is a p-divisible group.

[1] A complete field K with these properties is called a *perfectoid* field.

(b) Infer from (a) that $\mathfrak{m} = \mathfrak{m}^2$, and conclude that R is not Noetherian (**Hint**: Krull's intersection theorem).

MATH 204B, WINTER [redacted]

NUMBER THEORY II, HW 4

[redacted]

From Neukirch's book `Algebraic Number Theory`:

- Exercises:

  7 on page 115; 1 and 2 on pages 165–166

Problem A. Let K be a field equipped with a non-archimedean absolute value $|\cdot|$ which we assume is non-trivial. We endow the vector space of polynomials $K[t]$ with the norm $\|\cdot\|$ defined as follows.

$$\|f\| = \max\{|a_0|, |a_1|, \dots, |a_n|\} \qquad f = a_0 + a_1 t + \cdots + a_n t^n.$$

(a) Show that $\|\cdot\|$ is multiplicative; meaning that $\forall f, g \in K[t]$ we have

$$\|fg\| = \|f\| \cdot \|g\|.$$

(`Hint`: Adapt the proof of the Gauss Lemma about contents.)

(b) Check that $\|\cdot\|$ extends uniquely to an absolute value on the field $K(t)$ of rational functions.

(c) Is $K(t)$ complete? Prove it or give a divergent Cauchy sequence.

Problem B. Consider the field $F = \mathbb{F}_p(t)$ with the absolute value $|\cdot|_t$ and its completion $\hat{F} = \mathbb{F}_p((t))$; the field of formal Laurent series over $\mathbb{F}_p$.

(a) Argue that F is countable but $\hat{F}$ is uncountable. Deduce that $\hat{F}$ is not an algebraic extension of F.

(b) Choose an element $\gamma \in \hat{F}$ which is transcendental over F and let

$$E = F(\gamma) \qquad K = F(\gamma^p).$$

Observe that the field extension E/K is purely inseparable of degree p.

(c) Show that E and K have the same closures in $\hat{F}$. More precisely that

$$\hat{K} = \hat{E} = \hat{F}.$$

(This example shows that it can happen that a non-trivial field extension collapses upon completion.)

MATH 204B, WINTER [redacted]

NUMBER THEORY II, HW 5

[redacted]).

From Neukirch's book `Algebraic Number Theory`:

- Exercises:

  2 on page 152 (take K complete); 1 on page 159; 3 on page 166

Problem A. Let $(K, |\cdot|)$ be a complete non-archimedean field, and suppose E/K is a finite extension with separable residual extension k_E/k_K.

(a) Check that E/K Galois $\Longrightarrow$ k_E/k_K Galois.

(b) Assuming E/K is Galois show that the canonical homomorphism

$$\psi : \mathrm{Gal}(E/K) \longrightarrow \mathrm{Gal}(k_E/k_K)$$

is surjective and $E^{\ker(\psi)}$ is the maximal unramified extension of K in E.

Problem B. Let $p^r > 1$ be a prime power, and let ζ be a primitive p^r-th root of unity in $\bar{\mathbb{Q}}_p$.

(a) Explain why $\mathbb{Q}_p(\zeta)$ is a totally ramified extension of $\mathbb{Q}_p$ of degree $\phi(p^r)$, and the element $1-\zeta$ is a uniformizer of $\mathbb{Q}_p(\zeta)$.

(b) Let $r = 1$. Prove the following identity.

$$\mathbb{Q}_p(\zeta) = \mathbb{Q}_p(\sqrt[p-1]{-p}).$$

(`Hint`: Write $p = u(1-\zeta)^{p-1}$ with a unit $u \equiv -1 \bmod (1-\zeta)$ by Wilson's congruence. Hensel's lemma shows $-u = x^{p-1}$ for some $x \in \mathbb{Q}_p(\zeta)$. Consequently $-p$ is also a $(p-1)$-st power.)

MATH 204B, WINTER [redacted]

NUMBER THEORY II, HW 6

[redacted]).

From Neukirch's book `Algebraic Number Theory`:

- Exercises:

  3 on page 159 (assume L/K are local fields); 3 on page 176

Problem A. Here we show $\bar{\mathbb{Q}}_p$ is <u>not</u> complete relative to $|\cdot|_p$.

(a) Let $\mathbb{Q}_{p^{n!}}$ be the unramified extension of $\mathbb{Q}_p$ of degree $n!$. (From class we know that $\mathbb{Q}_{p^{n!}} = \mathbb{Q}_p(\xi_n)$ where $\xi_n \in \bar{\mathbb{Q}}_p$ is a primitive $(p^{n!}-1)$-st root of unity.) Check that $\mathbb{Q}_{p^{n!}} \subset \mathbb{Q}_{p^{(n+1)!}}$ for all n.

(b) Let s_n be the n-th partial sum of the infinite series $\sum_{i=0}^{\infty} \xi_i p^i$. Verify that $s_n \in \mathbb{Q}_{p^{n!}}$, and that the sequence $(s_n)_{n\in\mathbb{N}}$ is Cauchy in $\bar{\mathbb{Q}}_p$.

(c) Suppose $s_n \to \alpha \in C$. Use Krasner's Lemma to see that $\mathbb{Q}_p(s_n) = \mathbb{Q}_p(\alpha)$ for all n sufficiently large. Deduce that $\alpha \in \mathbb{Q}_{p^{n!}}$ for such n.

(d) Fix a large n as in (c) and argue that α has a p-expansion $\alpha = \sum_{i=0}^{\infty} c_i p^i$ in $\mathbb{Q}_{p^{n!}}$ whose coefficients are either 0 or powers of ξ_n.

(e) For $m > n$ compare the two expansions of α modulo p^{m+1} and infer that $\xi_i = c_i$ for all $i \leq m$. (Observing that $\langle \xi_i \rangle \subset \langle \xi_m \rangle$ may be helpful.)

(f) Get the contradiction $\mathbb{Q}_{p^{m!}} = \mathbb{Q}_{p^{n!}}$.

Problem B. In continuation of Problem A we show that the p-adic completion $\mathbb{C}_p = \hat{\bar{\mathbb{Q}}}_p$ is algebraically closed.

(a) Let $f \in \mathbb{C}_p[X]$ be monic and irreducible. Spell out why $\forall \delta > 0$ there is a monic polynomial $g \in \bar{\mathbb{Q}}_p[X]$ of the same degree such that $\|f - g\| < \delta$.

(b) As explained in class this implies g is irreducible if δ is small enough, and that g moreover has the root exchange property: For any root $\alpha \in \bar{\mathbb{C}}_p$ of f there is a root $\beta \in \bar{\mathbb{C}}_p$ of g such that $\mathbb{C}_p(\alpha) = \mathbb{C}_p(\beta)$.

   – conclude that $\alpha \in \mathbb{C}_p$.

Problem C. (Will not be graded.) Let K be a non-archimedean local field with valuation ring R, and normalized[1] absolute value $\|\cdot\|_K$. Let μ be the Haar measure on K with $\mu(R) = 1$. Show that $\mu(xR) = \|x\|_K$ for all $x \in K$.

[1]That is $\|x\|_K = q^{-v_K(x)}$ where q is the size of the residue field.

MATH 204B, WINTER [redacted]

NUMBER THEORY II, HW 7

[redacted]).

From Neukirch's book `Algebraic Number Theory`:

- Exercises:

  2, 4, 5 on page 142

Problem A. Here we show that $\mathbb{Q}_p$ has only finitely many extensions of a given degree (in a fixed algebraic closure $\bar{\mathbb{Q}}_p$).

(a) Reduce the question to showing that any finite extension $K/\mathbb{Q}_p$ only has finitely many totally ramified extensions E/K of a given degree n.

(b) As shown in class any such E/K is of the form $E = K(\Pi)$ where $\Pi \in E$ is a uniformizer. Furthermore the minimal polynomial of Π is an Eisenstein polynomial:

$$f(X) = X^n + \pi a_{n-1} X^{n-1} + \cdots + \pi a_1 X + \pi a_0, \qquad n = [E : K].$$

Here $\pi \in K$ is a choice of uniformizer; all $a_i \in R$ and $a_0 \in R^\times$.

– deduce that there is an n-to-one **map** from pairs (E, Π) onto $R^{n-1} \times R^\times$.

(c) Show that the inverse image of $(a_{n-1}, \dots, a_1, a_0)$ gives rise to the same fields E as the inverse image of any close enough tuple $(b_{n-1}, \dots, b_1, b_0)$. (`Hint`: Krasner's lemma; or rather a consequence thereof from class.)

(d) Using the compactness of $R^{n-1} \times R^\times$ deduce that there are only finitely many totally ramified E/K of degree n.

Problem B. Let k be any field of characteristic $p > 0$. Here we show that $K = k((t))$ has infinitely many separable extensions of degree p (in a fixed separable closure K^{sep}).

(a) Consider the rational functions $\frac{1}{t^n}$ with $n > 0$ prime-to-p. Suppose $n > n'$ and

$$\frac{1}{t^n} - \frac{1}{t^{n'}} = f^p - f, \qquad f \in K.$$

Argue that $f \notin k[\![t]\!]$ – in other words that $v_K(f) < 0$.

(b) In continuation of (a) check that

$$-n = v_K(f^p - f) = \min\{v_K(f^p), v_K(f)\} = pv_K(f)$$

which contradicts the assumption $p \nmid n$.

(c) Conclude that K has infinitely many p-extensions in K^{sep}. (`Hint:` Use Artin-Schreier theory. By (b) the additive group $K/\wp(K)$ is infinite, where $\wp(f) = f^p - f$ is the Artin-Schreier operator $\wp : K \to K$.)

(d) Assuming k is finite (so that K is a local field) adapt the strategy of Problem A to show that K has only finitely many **tamely** ramified extensions in K^{sep} of any given degree. (`Hint:` Separability of Eisenstein polynomials is what allows you to use Krasner's lemma.)

MATH 204B, WINTER [redacted]

NUMBER THEORY II, HW 8

[redacted]).

From Neukirch's book `Algebraic Number Theory`:

- Exercises:

  1 on page 142 (note that $\frac{1}{1-p}$ *should be* $\frac{1}{p-1}$ *here.* ***Hint:*** *Set* $\log(p) = 0$*)*

Problem A. (This exercise should have been assigned weeks ago.) Let E/K be a finite extension of local fields with uniformizers π and Π. Thus $\pi \sim \Pi^e$ where $e = e(E/K)$ is the ramification index. Let $f = f(E/K)$ be the inertia degree.

(a) Suppose $\beta_1, \dots, \beta_r$ are elements of R_E whose reductions modulo π span $R_E/\pi R_E$ as a k-vector space ($k = R/\pi R$). Show that $\beta_1, \dots, \beta_r$ generate R_E as an R-module. (`Hint:` $R_E = M + \pi R_E$ where $M = R\beta_1 + \cdots + R\beta_r$.)

(b) Suppose $\alpha_1, \dots, \alpha_f$ are elements of R_E whose reductions modulo Π form a k-basis for k_E. Using part (a) show that the set of elements

$$\alpha_i \Pi^j \qquad (i = 1, \dots, f \qquad j = 0, \dots, e-1)$$

form an R-basis for R_E.

(c) Conclude that R_E is a free R-module of rank $[E : K]$.

Problem B. Let E/K be a finite Galois extension of local fields with Galois group $G = \mathrm{Gal}(E/K)$ and higher ramification groups

$$G_i = \{\sigma \in G : v_E\big(\sigma(x) - x\big) > i \;\; \forall x \in R_E\}.$$

Our goal is to show $G_i = \{1\}$ for all sufficiently large i.

(a) Suppose $x_1, \dots, x_r$ generate R_E as an R-module (cf. Problem A). Check that $\sigma \in G$ lies in the ith ramification group G_i if and only if

$$v_E\big(\sigma(x_s) - x_s\big) > i \qquad \forall s = 1, \dots, r.$$

(b) Choose an $N \in \mathbb{N}$ bigger than all finite valuations $v_E(\sigma(x_s) - x_s)$ where $\sigma \in G$ and $s = 1, \dots, r$ vary. Argue that

$$G_i = \{1\} \qquad \forall i \geq N.$$

(`Hint:` $\sigma \in G_N$ must fix all the x_s since $v_E(\sigma(x_s) - x_s)$ would have to be infinite.)

(c) Fill in the details of the following alternative argument: Since G is finite the G_i become stationary. Furthermore $\bigcap_{i>0} G_i = \{1\}$ since an element thereof acts trivially on $R_E = \varprojlim R_E/\mathfrak{m}_E^{i+1}$. Thus $G_i = \{1\}$ for $i >> 0$.

Problem C. Let $\mathbb{Q}_p^{\mathrm{ur}}$ be the maximal unramified extension of $\mathbb{Q}_p$ in some fixed algebraic closure $\bar{\mathbb{Q}}_p$.

(a) Why is $\mathbb{Q}_p^{\mathrm{ur}}$ <u>not</u> complete? (Use Problem A on HW6.)

(b) Show that its completion $\widehat{\mathbb{Q}_p^{\mathrm{ur}}} \subset \mathbb{C}_p$ has a valuation ring $\widehat{\mathbb{Z}_p^{\mathrm{ur}}}$ which is complete, with p as a uniformizer, and it has residue field[1]

$$\widehat{\mathbb{Z}_p^{\mathrm{ur}}}/(p) \xrightarrow{\sim} \bar{\mathbb{F}}_p.$$

(c) Prove that $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p)$ is topologically generated by Frobenius (i.e., the subgroup generated by the Frobenius automorphism is dense):

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \xrightarrow{\sim} \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) = \hat{\mathbb{Z}}.$$

(Here $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ is the profinite completion of the integers.)

Problem D. Let $\mathbb{Q}_p^{\mathrm{tr}} \supset \mathbb{Q}_p^{\mathrm{ur}}$ be the union of all tamely ramified finite extensions of $\mathbb{Q}_p$ in some fixed algebraic closure $\bar{\mathbb{Q}}_p$.

(a) For each $n > 0$ let $\pi_n \in \bar{\mathbb{Q}}_p$ be a root of the polynomial $X^{p^n-1} + p$. Show that $\mathbb{Q}_{p^n}(\pi_n)$ is a totally and tamely ramified degree $p^n - 1$ extension of $\mathbb{Q}_{p^n}$ – which is independent of the choice of root π_n.

(b) Deduce that $\mathbb{Q}_{p^n}(\pi_n)$ is the splitting field of $X^{p^n-1}+p \in \mathbb{Z}_{p^n}[X]$ (therefore Galois) with Galois group

$$\mathrm{Gal}(\mathbb{Q}_{p^n}(\pi_n)/\mathbb{Q}_{p^n}) \xrightarrow{\sim} \mu_{p^n-1}(\bar{\mathbb{Q}}_p) \xrightarrow{\sim} \mathbb{F}_{p^n}^\times.$$

(Send σ to the ratio $\frac{\sigma(\pi_n)}{\pi_n}$ and then reduce modulo p.)

[1] Meaning $\widehat{\mathbb{Z}_p^{\mathrm{ur}}}$ is the ring of Witt vectors $W(\bar{\mathbb{F}}_p)$ of the characteristic p perfect field $\bar{\mathbb{F}}_p$.

(c) For $n = 1$ observe that $\mathbb{Q}_p(\pi_1) = \mathbb{Q}_p(\zeta_p)$. (Use Problem B on HW5.)

(d) Verify that $\mathbb{Q}_p^{\mathrm{tr}} = \bigcup_{n>0} \mathbb{Q}_{p^n}(\pi_n)$ and conclude that there is an isomorphism of topological groups

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tr}}/\mathbb{Q}_p^{\mathrm{ur}}) \xrightarrow{\sim} \varprojlim \mathbb{F}_{p^n}^\times$$

where the transition map $\mathbb{F}_{p^n}^\times \to \mathbb{F}_{p^m}^\times$ is the norm map for $m|n$.

(e) Infer that $P = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{tr}})$ is the unique Sylow pro-p subgroup (meaning the largest pro-p subgroup) of the inertia group $I = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{ur}})$.

(`Hint`: Let P be any maximal pro-p subgroup. Try to show $\mathbb{Q}_p^{\mathrm{tr}} = \bar{\mathbb{Q}}_p^P$. The inclusion $\subset$ essentially follows from (d). For $\supset$ observe that $\bar{\mathbb{Q}}_p^P$ is the smallest subfield of $\bar{\mathbb{Q}}_p$ with a pro-p Galois group.)

MATH 204B, WINTER [redacted]

NUMBER THEORY II, HW 9

[redacted]).

From Neukirch's book `Algebraic Number Theory`:

- Exercises:

  1 on page 181

  (`Hint`: Recall that a $\sigma \in G_0$ lies in G_i if and only if $v\big(\sigma(\Pi)/\Pi - 1\big) \geq i$. Taking $\Pi = \zeta - 1$ reduces the problem to reading off the valuation $v(\zeta^N - 1)$ from the p-expansion of N.)

Problem A. Let K be a field, and let $\mathrm{Gal}_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be its absolute Galois group (with the Krull topology).

(a) Show that $\mathrm{GL}_n(\mathbb{C})$ has "no small subgroups" – meaning the identity matrix I has an open neighborhood which does not contain any non-trivial subgroup.

(`Hint`: First do this for $\mathbb{C}^\times$. In general, if $\|A - I\| < \epsilon$ then all eigenvalues λ of A satisfy $|\lambda - 1| < \epsilon$. Therefore, if all powers A^N also lie in the ϵ-ball we must have $\lambda = 1$, i.e. A is at least unipotent. However, since the A^N remain bounded we conclude that $A = I$.)

(b) Deduce from (a) that any continuous representation $\mathrm{Gal}_K \to \mathrm{GL}_n(\mathbb{C})$ factors through $\mathrm{Gal}(E/K)$ for some finite Galois extension E/K. When $n = 1$ check that one can take E/K to be an abelian extension.

(c) Let $n = 1$ and suppose K is a non-archimedean local field. Explain why composition with the Artin map ϕ_K defines a bijection

$$\{\text{continuous characters } \mathrm{Gal}_K \to \mathbb{C}^\times\} \overset{1:1}{\longleftrightarrow}$$
$$\{\text{continuous characters } K^\times \to \mathbb{C}^\times \text{ of } \textbf{finite} \text{ order}\}.$$

(It sends $\chi \mapsto \chi^{\mathrm{ab}} \circ \phi_K$ where χ^{ab} is the character of $\mathrm{Gal}_K^{\mathrm{ab}}$ given by χ.)

Problem B. Let $K/\mathbb{Q}_p$ be a finite extension, with absolute Galois group Gal_K. The cyclotomic character $\chi_{\mathrm{cyc}} : \mathrm{Gal}_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$ is the projection onto

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) = \varprojlim \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \simeq \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

Its restriction to $\mathrm{Gal}_K \subset \mathrm{Gal}_{\mathbb{Q}_p}$ will also be denoted by χ_{cyc}.

(a) Check that $\chi_{\mathrm{cyc}} : \mathrm{Gal}_K \to \mathbb{Z}_p^\times$ is continuous, but <u>not</u> of finite order.

(b) Consider the composition $\chi_{\mathrm{cyc}}^{\mathrm{ab}} \circ \phi_K$, which is the character $K^\times \to \mathbb{Z}_p^\times$ corresponding to χ_{cyc} via class field theory. Verify that

$$(\chi_{\mathrm{cyc}}^{\mathrm{ab}} \circ \phi_K)(x) = N_{K/\mathbb{Q}_p}(x) \cdot \|x\|_K \qquad \forall x \in K^\times$$

where $\|\cdot\|_K$ is the normalized absolute value on K.

(`Hint`: Reduce to the case $K = \mathbb{Q}_p$ utilizing that Artin maps are compatible with norm maps. To see that $p \mapsto 1$ write p as a norm from $\mathbb{Q}_p(\zeta_{p^n})$. Finally check that a unit $u \in \mathbb{Z}_p^\times$ is mapped to itself using $\mathbb{Z}_p^\times \xrightarrow{\sim} I_{\mathbb{Q}_p}^{\mathrm{ab}}$.)

Problem C. Let K be a non-archimedean local field. The Weil group $W_K \subset \mathrm{Gal}_K$ consists of the automorphisms which act as $\mathbb{Z}$-powers of Frobenius on the residue field. Thus it sits in a short exact sequence

$$0 \longrightarrow I_K \longrightarrow W_K \longrightarrow \mathbb{Z} \longrightarrow 0 \tag{1}$$

where $I_K = \mathrm{Gal}_{K^{\mathrm{ur}}}$ is the inertia subgroup. (Compare this to the short exact sequence

$$0 \longrightarrow I_K \longrightarrow \mathrm{Gal}_K \longrightarrow \hat{\mathbb{Z}} \longrightarrow 0$$

where $\hat{\mathbb{Z}} \simeq \mathrm{Gal}_k = \overline{\langle \mathrm{Frob} \rangle}$ is the absolute Galois group of the residue field k.)

(a) Endow I_K with the Krull topology. Prove that there is a unique topology on W_K which makes (1) a short exact sequence of **topological** groups (meaning all maps are continuous and $W_K/I_K \xrightarrow{\sim} \mathbb{Z}$ is a homeomorphism.)

(`Hint`: As a neighborhood basis at the identity take all $\mathrm{Gal}_E \subset I_K$ where E/K^{ur} is a varying finite extension.)

(b) Show that W_K is a dense subgroup of Gal_K, but the topology on W_K defined in (a) is **stronger** than the induced topology from Gal_K.

(c) Verify that the Artin map ϕ_K defines a topological isomorphism

$$K^\times \xrightarrow{\sim} W_K^{\mathrm{ab}}.$$

(Here $K^\times$ carries the standard topology defined by $\|\cdot\|_K$.)

Problem D. Thank you all for a great quarter! Please fill out your CAPE teaching evaluations (due Monday March 18th at 8AM).

MATH 204B, WINTER [redacted]

NUMBER THEORY II, FINAL [redacted]

[redacted].

Problem A. Let $p \equiv 1 \pmod 3$ be a prime number.

(a) Show that every cubic Galois extension $E/\mathbb{Q}_p$ is of the form $E = \mathbb{Q}_p(\sqrt[3]{\theta})$ for some $\theta \in \mathbb{Q}_p^\times$ (not in $\mathbb{Q}_p^{\times 3}$) – and vice versa.

(b) How many cubic Galois extensions E does $\mathbb{Q}_p$ have (inside a fixed algebraic closure)? Are they all tamely ramified?

Problem B.

(a) Does the additive group $\mathbb{Q}_p$ have a maximal compact subgroup?

(b) Show that $\mathbb{Z}_p^\times$ is the unique maximal compact subgroup of $\mathbb{Q}_p^\times$. Generalize this statement – and your argument – to finite extensions of $\mathbb{Q}_p$.

(c) Let $G \subset \bar{\mathbb{Q}}_p^\times$ be a compact subgroup. Prove that G is contained in the units U_K for some finite extension $K/\mathbb{Q}_p$. (`Hint`: Write G as a countable union of closed subsets $G \cap K^\times$ and use that G is a Baire space.)

Problem C. Let K be a non-archimedean local field with valuation v_K (which extends uniquely to an algebraic closure $\bar{K}$). Let

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in K[X]$$

be a polynomial with nonzero leading and constant coefficients; $a_0 a_n \neq 0$.

(a) Suppose the roots $\alpha_1, \ldots, \alpha_n \in \bar{K}$ of f have distinct (finite) valuations

$$v_K(\alpha_1) > v_K(\alpha_2) > \cdots > v_K(\alpha_n).$$

Check that all $a_i \neq 0$ and join the points $P_i = \big(i, v_K(a_i)\big)$ in the plane by a piecewise linear segment. Show that the **slopes** of this convex segment are precisely $-v_K(\alpha_i)$ for $i = 1, \ldots, n$.

(b) Extend the result from (a) to the general case without assumptions on the $v_K(\alpha_i)$ (allowing distinct roots to have the same valuation).

Hint: Consider the "lower convex hull" of the set of points P_i. It might be helpful to do the case $n = 2$ first.

Problem D. A quaternion algebra D over $\mathbb{Q}_p$ admits a basis $\{1, i, j, k\}$ satisfying the relations

$$i^2 = a \qquad j^2 = b \qquad ij = k = -ji$$

for some $a, b \in \mathbb{Q}_p^\times$. (This follows easily from the Skolem-Noether theorem.)

(a) When $a = 1$ show that there is an isomorphism $D \xrightarrow{\sim} M_2(\mathbb{Q}_p)$ given by

$$1 \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \qquad i \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \qquad j \mapsto \left(\begin{smallmatrix} 0 & b \\ 1 & 0 \end{smallmatrix}\right) \qquad k \mapsto \left(\begin{smallmatrix} 0 & b \\ -1 & 0 \end{smallmatrix}\right).$$

(b) Show that D contains at least the following three quadratic subfields:

$$\mathbb{Q}_p(\sqrt{a}) \qquad \mathbb{Q}_p(\sqrt{b}) \qquad \mathbb{Q}_p(\sqrt{-ab}).$$

Deduce that $\mathbb{Q}_{p^2} \subset D$ (where $\mathbb{Q}_{p^2}$ is the unramified quadratic extension).

(c) Prove that the following five conditions are equivalent:

(1) D is isomorphic to the matrix algebra $M_2(\mathbb{Q}_p)$.

(2) D is not a division algebra.

(3) There is a nonzero $q \in D$ with norm $N(q) = q\bar{q} = 0$.

(4) The element a lies in the norm group of $\mathbb{Q}_p(\sqrt{b})$.

(5) $(a, b)_2$=1, where $(\cdot, \cdot)_2$ denotes the Hilbert symbol – that is the pairing

$$\mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \longrightarrow \{\pm 1\} \qquad (a, b)_2 = \phi_{\mathbb{Q}_p}(a)(\sqrt{b})/\sqrt{b}.$$

(Here $\phi_{\mathbb{Q}_p}$ is the Artin map.)

Hints: For (1) $\Longleftrightarrow$ (2) just apply Wedderburn's theorem. For the implication (5) $\Longrightarrow$ (1) suppose $b^{-1} = N(r + s\sqrt{a})$ – then introduce the elements $u = rj + sk$ and $v = (1 + a)i + (1 - a)ui$ and refer to part (a).

(d) Note that your arguments in (c) work for any finite extension of $\mathbb{Q}_p$ and conclude that there is an isomorphism

$$D \otimes_{\mathbb{Q}_p} K \xrightarrow{\sim} M_2(K)$$

where $K \subset D$ is any of the three quadratic subfields from part (b).

Problem E. Let p be a prime. A "strict p-ring" is a p-adically complete p-torsion-free ring R for which $R/(p)$ is perfect (meaning the p-power Frobenius map $\varphi : R/(p) \longrightarrow R/(p)$ sending $x \mapsto x^p$ is a bijection).

(a) For such R check that $R/(p)$ is necessarily reduced (has no nonzero nilpotents).

(b) If $K/\mathbb{Q}_p$ is a finite extension, deduce that its valuation ring $\mathcal{O}_K$ is a strict p-ring if and only if $K/\mathbb{Q}_p$ is unramified.

(c) Prove that the projection map $\pi : R \longrightarrow R/(p)$ admits a **unique** multiplicative section $[\bullet] : R/(p) \longrightarrow R$ (known as the "Teichmüller map").

(Hint: For each n choose a lift $x_n \in R$ of $\varphi^{-n}(\bar{x})$. If s is a multiplicative section of the projection ($\pi \circ s = \mathrm{Id}$) show that $s(\bar{x}) = \lim_{n\to\infty} x_n^{p^n}$.)

(d) Show that every element $x \in R$ has a "Teichmüller expansion"

$$x = \sum_{n=0}^{\infty} [\bar{a}_n] \cdot p^n$$

for a **unique** sequence of coordinates $\bar{a}_0, \bar{a}_1, \bar{a}_2, \dots$ in $R/(p)$.

(Fact: One can show that the functor $R \rightsquigarrow R/(p)$ is an equivalence between the category of strict p-rings and that of perfect rings of characteristic p. Given a perfect ring $\mathcal{R}$ there is a natural choice of a strict p-ring known as the ring of Witt vectors $W(\mathcal{R})$. For instance $W(\mathbb{F}_p) = \mathbb{Z}_p$ and $W(\bar{\mathbb{F}}_p) = \widehat{\mathbb{Z}_p^{\mathrm{ur}}}$, cf. Problem C on HW8.)